

REMARKS

Reconsideration and allowance of the subject application are respectfully requested.

Claims 1-18 are pending.

The specification has been amended as requested by the Examiner.

The Examiner makes an obviousness-type double patenting rejection of claims 1-6 in view of U.S. Patent No. 6,233,337 combined with Reeds (EP 0532228). Applicants have submitted, concurrently herewith, a terminal disclaimer with respect to U.S. Patent No. 6,233,337; thus rendering this rejection moot.

The Examiner makes an obviousness-type double patenting rejection of claims 1-18 in view of claim 1 in U.S. Application No. 09/124,300, now U.S. Patent 6,337,687. Applicants have submitted, concurrently herewith, a terminal disclaimer with respect to U.S. Patent 6,337,687; thus rendering this rejection moot.

Claims 1-5 stand rejected under 35 U.S.C. § 103 as being unpatentable over Reeds (EP 0532228) in view of Laufer (Discrete Mathematics and Applied Modern Algebra). Applicants respectfully traverse this art grounds of rejection.

The Examiner asserts that Reeds discloses the claimed invention except for the use of table lookup to evaluate involutions, and cites Laufer as making up for this deficiency. The cryptographic methodology employed by Reeds is disclosed principally in column 11 of Reeds. As the Examiner correctly notes, Reeds does disclose the use of a tbox function in this cryptographic

RECEIVED

methodology (see lines 20-25 and 30-34 of column 11). However, there is no disclosure in Reeds of "the inputs to the enhanced tbox function being subjected to a permutation using one or more of the secret offsets to produce a permutation result," as recited in claim 1. Clearly, the discrete mathematics taught in Laufer do not overcome the deficiencies of Reeds.

Accordingly, Reeds in view of Laufer does not render claim 1 obvious to one skilled in the art. Claims 2-5, dependent upon claim 1, are patentable for the reasons stated above with respect to claim 1 as well as on their own merits.

In subsequent art grounds of rejection the Examiner also cites the teachings in Vernam, G. S., "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications," Journal A.I.E.E. Vol. XVI, pgs 109-115, Dec. 1926, and Takaragi et al. (U.S. Patent No. 5,222,139) in combination with Reeds in view Laufer in rejecting claim 6-7 and 7-18. However, none of these additionally cited references overcome the disclosure and suggested deficiencies discussed above with respect to claim 1. Consequently, claim 1 is patentable over the art cited by the Examiner. The remaining claims, alone or by their dependency upon claim 1, recite similar limitations to those discussed above with respect to claim 1, and are patentable at least for the reasons stated above with respect to claim 1.

The Examiner made these same rejections in now issued U.S. Patent 6,337,687, which included claims having at least the same limitations discussed above. Similar arguments to those presented above, were also presented in the '687 patent and resulted in the allowance of that patent.

Accordingly, Applicants are of the strong belief that the subject application is in condition for allowance.

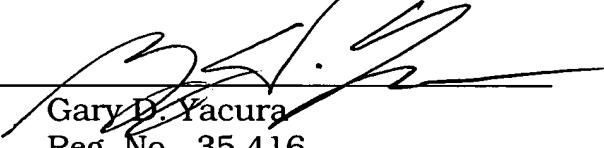
In the event that any outstanding matters remain in this application, Applicant requests that the Examiner contact the undersigned at the telephone number listed below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Very truly yours,

HARNESS, DICKEY & PIERCE, P.L.C.

By


Gary D. Yacura
Reg. No. 35,416

GDY:jcp

P.O. Box 8910
Reston, VA 20195
(703) 668-8000